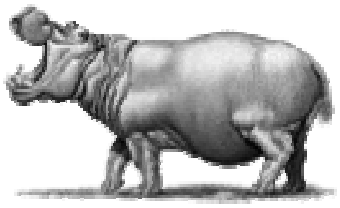
HEALTH SYSTEMS

PMO526

DEPARTMENT OF PREVENTIVE MEDICINE AND BIOMETRICS

# HIPAA: HEADACHE OR HEADWAY?




By

Chris Tabatzky

Amy M. Millikan

Sven T. Berg

Paul Ciminera

Stephen A. Felt

Kenneth O. Jacobsen

Nancy L. Merrill


A Paper Submitted by Group Archaic to the Faculty

Discussing Current Issues of Healthcare Delivery

In Partial Fulfillment of Course Requirements


Uniformed Services University of the Health Sciences

Bethesda, MD


29 October 2002

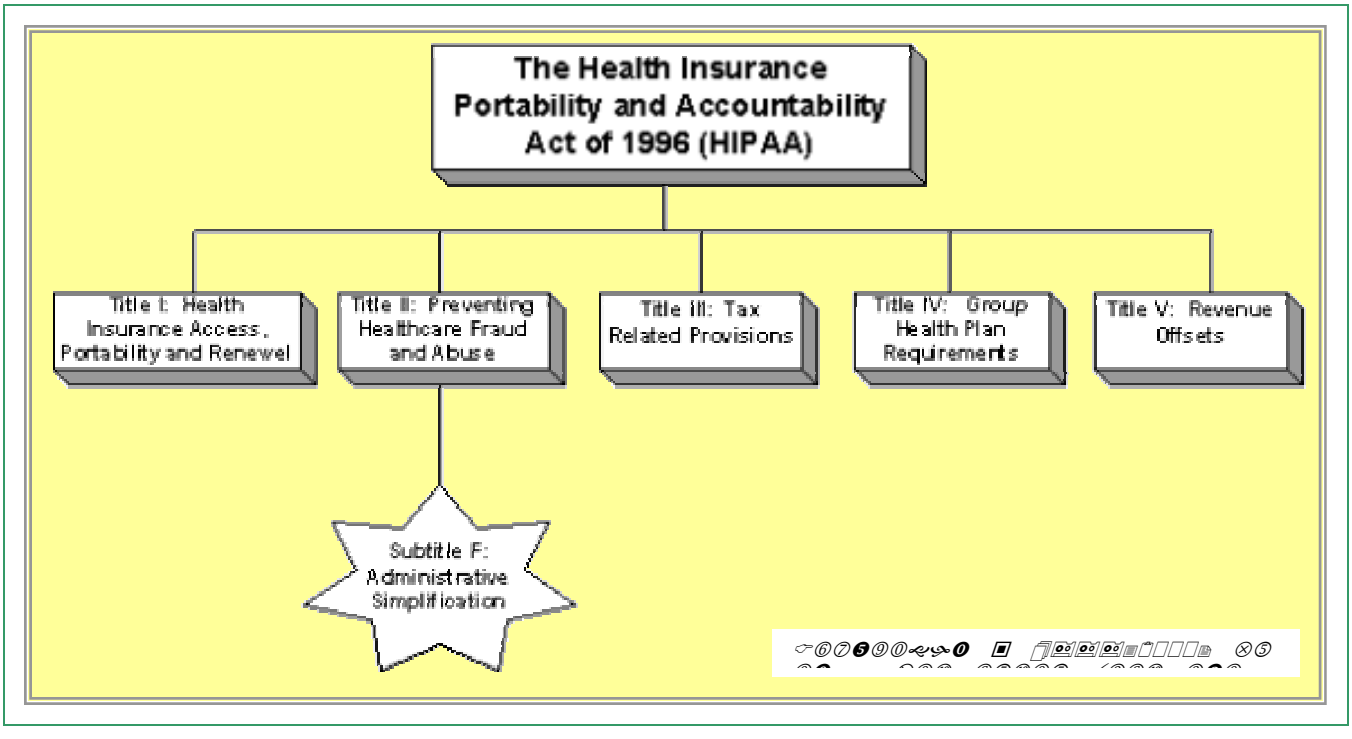
Introduction

The Health Insurance Portability and Accountability Act (HIPAA) was signed into law by President Clinton on August 21, 1996. Also known as the Kennedy-Kassebaum Act (Public Law 104-191), this legislation was designed to address a broad range of healthcare issues. HIPAA aimed to: (1) improve the portability of health insurance coverage in the group and individual markets, (2) limit healthcare fraud and abuse, (3) promote the use of medical savings accounts, (4) improve patients' access to long-term care and (5) simplify the administration of health insurance.

The last objective, defined as Administrative Simplification, is arguably the most significant piece of healthcare legislation since Lyndon Johnson recognized "The Great Society" and created Medicare in 1965. The intent of HIPAA is to improve the efficiency and effectiveness of the healthcare system by encouraging the development of health information systems that utilize electronic data interchange (EDI). More importantly, HIPAA seeks to establish and require the use of national standards when performing these healthcare transactions between organizations electronically.

Within this framework, HIPAA required Congress to craft a Patient Privacy Bill but in the absence of such a bill, HIPAA tasked DHHS to define rules for the protection of Patient Information. These rules are to be applied through security standards, policies, and practices that all entities must implement who use, store, maintain, or transmit patient health information. Specifically, healthcare providers, payers, clearinghouses, billing agents, third-party administrators, and so on are all affected by the requirements of administrative simplification and patient privacy.

*Legislative Organization: HIPA consists of five titles (see below). Administrative Simplification falls under title II, Subtitle F.*



HIPAA impacts all health care organizations, hospitals, physicians' offices, health plans, employers, public health authorities, life insurers, clearinghouses, billing agencies, information systems vendors, service organizations and universities. Under the law, affected organizations are termed: **Covered Entities**. HIPAA is rapidly becoming a major issue in health care for a number of reasons:

- The implementation timeframe is short—only 24 months for most organizations.
- The standards were only recently settled, so organizations have just begun to focus on how to achieve HIPAA compliance.
- HIPAA imposes significant financial, criminal and civil penalties for non-compliance. Organizations face serious liability risks for unauthorized disclosure of patient health data.
- Becoming HIPAA compliant is a complex and daunting task due to the sweeping reach of the regulations.

Group $A_{rchaic}$ sequentially examined the major components of HIPAA Title II, subtitle F, specifically Administrative Simplification and the Privacy Rule. The impact of these provisions on healthcare providers, administrators and consumers (patients) was discussed. A synopsis of these components and pertinent group discussion follows in outline form.

## Historical and Political Context

*In the early 1990's, the Bush Administration assembled leaders in the health care industry to advise on how administrative costs could be reduced. The group concluded that this could best be accomplished by increasing the use of electronic data interchange (EDI) within the industry. This advisory panel subsequently became known as WEDI-- the Workgroup for Data Interchange. WEDI went on to make the seminal recommendation that federal legislation be passed to ensure that a consistent set of standards could be used across all states—a recommendation that was incorporated into the 1993 Clinton Health Security Act. Although Congress failed to pass the Clinton Health care plan, likeminded legislation was reborn with passage of the Kennedy-Kassebaum Act in 1996. In fact, a substantial portion of HIPAA was lifted directly from the Clinton Act.*

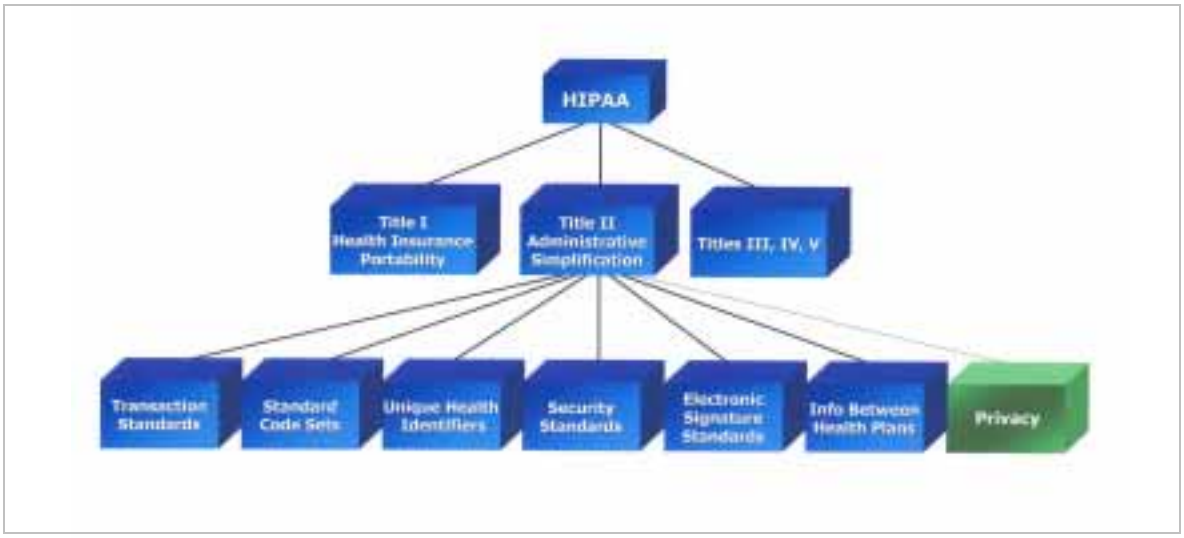
## Title II: Preventing Health Care Fraud and Abuse

### I Administrative Simplification

The Department of Health and Human Services (DHHS) considers the…

> "Administrative Simplification [of HIPAA]… to be the most significant healthcare law to create sweeping changes in the health industry since Medicare."

The major components of Administrative Simplification are represented below:






*Used with permission, Lisa L. Dahm, JD*

A. Electronic Health Transaction Standards and Code Sets

Currently, different health care providers and health plans use diverse electronic formats for data entry. DHHS estimates approximately 400 different formats are in use today just for health care insurance claim forms. It is estimated that more than $.20 of every healthcare dollar is spent on administrative overhead, with an additional $.11 of every healthcare dollar spent fraudulently. When fully implemented, it is conservatively estimated that HIPAA transactions will save providers $9 billion annually.

HIPAA requires the use of specific electronic formats developed by the American National Standards Institute (ANSI) for the following transactions:

a. health claims and equivalent encounter information
b. enrollment and dis-enrollment in a health plan
c. eligibility for a health plan
d. health care payment and remittance advice
e. health plan premium payments
f. health claim status
g. referral certification and authorization
h. coordination of benefits

HIPAA does not mandate the electronic exchange of *all* health care data. It establishes standard formats to be used when communicating specific health care transactions electronically. HIPAA requires ANSI ASC x12N Syntax as the EDI format.

All health care providers and plans will be required to use a single standardized set of codes to describe diseases, injuries, and other health problems as well as their causes, symptoms and actions taken. The code sets currently approved by HIPAA include: ICD-10, CPT-4, HCPCS Level II, and CDT-2. HCPCS Level III, ("local codes" used by most States), are specifically not allowed.

Electronic Transaction Standards were the first rule promulgated by HHS. The compliance date set for most covered entities is **October 16, 2003**. Non-compliance results in fines and exclusion from the Medicare Program. HHS is actually prohibited from paying claims that are not electronically submitted after October 16, 2003. (Specific waivers apply).

*Group $A_{rchaic}$ identified several issues pertaining to standardized transactions and codes beginning with cost. The projected costs of implementation, staffing, training, retrofit, hardware/software, compliance audits (more watchers to watch the watchers), and research are substantial. This legislation presents a huge financial burden to all entities concerned. HIPAA appears to fly in the face of the "incrementalism" so characteristic of prior healthcare policy. Federal government should not impose industry standards without providing that industry with the means to implement them. If we really want successful reform in this area, then some level of federal subsidy or funding is requisite and fair. One mechanism might include tax credits for HIPAA compliance during roll-out.*

*Administrative Simplification places a disproportionate burden on small healthcare systems and physician practices. Larger, corporate entities will have some infrastructure, and some IT legacy to recruit, even if it isn't immediately compliant. Smaller entities are hard-pressed to remain competitive.*

*It was noted that information technology has not been rapidly accepted by physicians, partially because of being burned by the overinflated promises of past IT initiatives (e.g., DoD). More importantly, for such technology to be adopted, it should be patient-centered, I.e., benefit the patient, as opposed to benefiting the system. Standardized transactions appear to have more to do with the system than the patient, especially in the eyes of health care providers. More coding will cost more money—whether computed in physician, nurse or support staff time.*

*The reduction in administrative overhead and improved efficiency should translate into increased profitability however, implementation across various platforms is bound to challenge systems and create additional layers in complexity and organizational structure. Individual states are no longer be able to use "local codes" for Medicaid. Since most states have created local codes for procedures, drugs, provider types, and category of service—and these codes are drivers for many automated processes, payment algorithms and reports—they are faced with restructuring entire systems and/or subcontracting with clearinghouses. It is widely accepted that, "HIPAA will likely drain the pool of skilled resources even more that Y2K and the stress on Human Resources and budgets will increase as the implementation deadline approaches."* [1]

*Consumers (and taxpayers) will ultimately pay the price as the cost of doing business marches on.*

B. Unique Identifiers for Providers, Employers, Health Plans, Patients

Standard Unique Identifier for Employers: On May 31, 2002 HHS issued a final rule to standardize the identifying numbers assigned to employers in the health care industry by using the existing Employer Identification Number (EIN), which is assigned and maintained by the Internal Revenue Service. Businesses that pay wages to employees already have an EIN.

Currently health plans and providers may use different ID numbers for a single employer in their transactions, increasing the time and cost for routine activities such as health plan enrollments and health plan premium payments. Most covered entities must comply with the EIN standard by **July 30, 2004**.

Standard Unique Health Care Provider Identifier: In May 1998, HHS proposed standards to require hospitals, doctors, nursing homes and other health care providers to obtain a unique identifier when filing electronic claims with public and private insurance programs. Providers would apply for an identifier once and keep it if they relocated or changed specialties. Currently, health care providers are assigned different ID numbers by each different private health plan, hospital, nursing home and public program such as Medicare and Medicaid. These multiple ID numbers result in slower payments, increased costs and a lack of coordination. The Final rule is in clearance. Estimated publication date was summer 2002.

Standard Unique Health Plan Identifier: HHS is working to propose standards that would create a unique identifier for health plans, making it easier for health care providers to conduct transactions with different health plans. Notice of Proposed Rule Making (NPRM) estimated publication date was 08/02.

Unique Identifier for Individuals: Although HIPAA initially included a requirement for a unique personal health care identifier, HHS and Congress have put the development of such a standard on hold indefinitely. In 1998, HHS delayed any work on this standard until after comprehensive privacy protections were in place. Since 1999, Congress has adopted budget language to ensure no such standard is adopted without Congress' approval. HHS has no plans to develop such an identifier.

*Group $A_{rchaic}$ voiced concern regarding the very real threat of identity theft. The incidence of identity theft through the Internet is growing at an astonishing rate. The FTC's toll-free hotline, which was established so that consumers could report identity theft and obtain counseling to resolve identity theft issues, averaged over 1,000 calls/week during July and August 2000. At present, Congress has enacted some protection for consumers (e.g., limits of liability on credit card charges) and in most cases, a consumer will know when his/her credit card is being used inappropriately, since a monthly statement is received.*

*It was not clear that similar safeguards had been enacted for providers. And how will providers know if their provider "ID" has been co-opted by others? The obvious black market for provider identity theft would be for prescription drugs. What if employees are crafty enough to "shadow" provider transactions, inserting nicely compensated services? The burden of proof will be on the provider to establish that he/she did not, in fact, authorize a particular transaction on a particular date. Discovery may occur after years of transactions and this could mean a huge audit trail.*

*HIPAA will allow provider "profiling". The Feds and/or other entities will be able to assemble a portfolio on ALL provider billing activities—Medicare, Medicaid AND private insurance. This can be extrapolated to practice activities and methods of care. They will know how many patients you see, how old, how sick, how often and for how much-- who is performing abortions, who is not. Access to this information can have huge implications within the political powerbase.*

### C. Security of Health Information and Electronic Signature

The HIPAA security standard is designed to ensure confidentiality and integrity of individual health information. It requires a uniform level of protection of all health information that pertains to an individual. Unlike the electronic health transactions standards, which apply only to health data in electronic format, the security standards apply to all health care information that has been in an electronic form at any point in time. Patient information that has been faxed or emailed, for example, is subject to the HIPAA security standard. Specific rules apply to data that is stored or transmitted electronically.

The HIPAA security standard requires safeguards for physical storage and maintenance, transmission and access to individual health information. For electronic transmissions that use electronic signatures (which are not required), standards that ensure message integrity, user authentication and non-repudiation apply (identical to the financial transaction industry or electronic funds transfer). There are four aspects of the HIPAA security standard requirements:

- Information systems security: HIPAA requires the protection of all affected computers and data from compromise or loss.
- Physical security: HIPAA requires protection of all buildings, facilities and assets from compromise or threat.
- Audit trail: HIPAA requires health care providers to maintain audit trails of accesses to patient identifiable health information.
- Digital signature/data encryption: HIPAA requires transmission to be authenticated and protected from observation or change.

The final rule is being jointly developed by Centers for Medicare and Medicaid Services (CMS) and the Department of Commerce. CMS is attempting to link the privacy and security rules in light of the Privacy Rule modifications. Publication of

the Final rule is estimated 10/02 to 12/02. An electronic signature standard is on hold due to lack of consensus. Industry continues to work on this issue.

*Group $A_{rchaic}$ is fortunate to have members with considerable electronic engineering and security systems experience. Concern was raised as to the current capacity and knowledge base within the healthcare industry as it pertains to understanding and running security systems. Examples of publicly held security technologies include CERT and Standards for Trusted Systems. The current Federal Reserve System was built over many years with direct support and guidance by information security experts in the federal government (NSA). To expect healthcare providers operating within narrow financial margins, to acquire this security within a few years of regulation may be foolhardy.*

*The single most unpredictable factor in the security of any system is physical security. Breaks in physical security, be they access to the raw data or intentional sharing of the encryption technology, void the security of the system. In an electronic signature system, someone must be trusted to authenticate the signature "key". In most systems, a third party with very good physical security holds onto the prototype and is asked to verify the signature key. This of course requires standardization and cost sharing. It appears that HIPAA is struggling with these issues, and has avoided the use of electronic signatures to date.*

*Unfortunately, without electronic signatures and authentication, anyone can hop onto the network and pretend to be a node. They can steal or insert any codes or data they wish. Without third party authentication, security becomes a "common sense" practice problem. That is, hide your password, log off when not in use, deny access when business is closed, use firewalls with up to date virus software. These only provide low level security, however, and would not be acceptable for more intensive data processing. In processing protected health information (PHI) data, such limited measures may expose the operator to hefty fines.*

## II Privacy Rule

The Privacy Rule is a landmark comprehensive federal regulation that gives patients sweeping protections over the privacy of their medical records. The final regulation takes effect **April 14, 2003**. The fundamental principles that underlie the Privacy Rule include:

1. Ensure consumer control over their health information.
2. Establish guidelines for medical record use and release.
3. Ensure the security of personal health information.
4. Set accountability guidelines for medical record use and release.
5. Balance public responsibility with privacy protections.

***The Federal Register notes:***

*"In an era where consumers are increasingly concerned about the privacy of their personal information, the Privacy Rule creates for the first time, a floor of national protections for the privacy of their most sensitive information—health information.*

*Congress has passed other laws to protect consumers' personal information contained in bank, credit card, other financial records and even video rentals. These health privacy protections are intended to provide consumers with similar assurances that their health information, including genetic information, will be properly protected."*

The final Privacy Rule differs significantly from the draft version. Privacy regulations have undergone several rewrites since first issued in December 2000. Modifications were necessary to address serious unintended consequences of the original rule that would have interfered with patients' access to quality care. For example, patients would have been required to visit a pharmacy in person to sign paperwork before a pharmacist could review protected health information in order to fill their prescriptions. The Privacy Rule has been the subject of intense scrutiny from the general public and health care entities. HHS received more than 11,000 public comments on proposed modifications issued in March, 2002.

Key provisions to include Marketing, Use and Disclosure (Consent, Minimum Necessary, Incidental), Business Associates, and Limited Data Set are listed below.

A. Marketing

An authorization is required prior to using patient information for any marketing purposes. A covered entity is prohibited from selling lists of patients and enrollees to third parties or from disclosing protected health information (PHI) to a third party for the marketing activities of the third party without the individual's authorization. This does not include a face-to-face encounter. Doctors and other covered entities communicating with patients about treatment options or the covered entity's own health-related products and services are not considered marketing. For example, health care plans can inform patients of additional health plan coverage and value-added items or services, such as discounts for prescription drugs or eyeglasses.

The AMA has noted however that this prohibition would not prevent a covered entity from sending patients information on alternative treatments or therapies that benefit a third party in exchange for remuneration from the third party. It also appears that the marketing provision and the Privacy Rule will not cover many health-related web sites.

*Group $A_{rchaic}$ examined the marketing provision from the consumer perspective with particular attention to eHealth. Direct patient marketing appears to be a double-edged sword. The AMA has noted the fiduciary loophole, and concern was voiced over information asymmetry with "good" and "bad" marketing. It is clear that the Privacy Rule will not apply to many Internet health sites.*

*Survey after survey indicate that consumers are very concerned about privacy, ethical and security issues. There is confusion about whether personal health data disclosed on Internet sites is protected by law, and about who should regulate such information. Eighty-four percent of Internet users are concerned that businesses and/or people they do not know are getting personal information about them and their families.*[2] *Demographics also play a role in use patterns. In the US market, approximately 49% of Caucasians, 38% of African Americans, 37% of Asian Americans and 29% of Latinos seek health information online. (Cyber Dialogue)*

*Some of the most popular health Web sites are information-based. Since they only furnish health information and do not provide "healthcare" as it is defined by HIPAA, they do not fall within the federal regulation. Some sites offer additional services that require users to provide personal information as part of a "health assessment". Users may enter all sorts of information from height and weight to drug and alcohol use. This personal health information will not be protected by the privacy regulation. Some Web sites actually provide healthcare, but are still not covered by the regulation, because they do not accept health insurance. Only providers that process health claims electronically are covered by the regulation.*[3] *(see sidebar)*

*A Group $A_{rchaic}$ member noted that hospitals are also tapping into web marketing strategies—for example, setting up interactive web sites that will automatically remind female patients over 40 when it's time to come in for an annual breast cancer screening. This can lead to an increase in what hospitals call "incremental income". A Baltimore hospital has found that its Web site is the leading source of new customers for the stomach-stapling surgery it offers to very obese patients.*[5]

Rogue Pharmaceuticals:

The press has been filled with stories about rogue Web sites selling drugs without a legitimate prescription. Many of these pharmacists only conduct business online and specialize in drugs that treat sensitive or embarrassing conditions a patient may not wish to discuss with a doctor. Other sites provide online prescriptions for products that are not always easy to obtain, like the "morning after" pill. Sites such as these allow people to purchase a drug if they fill out a health assessment.--fees may even include an online "consultation" with a doctor. These sites do not accept health insurance requiring payment for the entire transaction via credit card. By refusing insurance, they are not "Covered Entities" as defined by HIPAA. Thus these sites remain outside the scope of the federal privacy regulation.

"Treatment" Sites

Some Web sites actually provide healthcare but are still not covered by the Privacy Rule because they do not accept health insurance. An example is online counseling. These sites tend to only accept credit cards. For example, at Cyberanalysis.com patients can make arrangements to communicate with participating doctors by cyber chat, email, videophone or telephone. An important point about this Web site is that it is not a referral service but an actual virtual counseling center that has analysts on staff. The critical question here is whether the Web site itself is a Covered Entity. Because it does not accept health insurance, the site and the counseling that takes place on the site would not be covered by the Privacy Rule.[4]

B. Use and Disclosure

Consent and Notice The most powerful change in the final version of the Privacy Rule has to do with patient consent. HHS has abandoned this requirement for use and/or disclosure of protected health information for treatment, payment and healthcare operations. Providers with a **direct** treatment relationship with their patients are no longer obligated to obtain consent. Certain restrictions apply.

In place of this consent, the regulation requires that direct health care providers must make a "good faith effort" to obtain a written acknowledgement from the patient that he/she has received notice of the provider's privacy practices. (Notice of Privacy Practices). This Notice must describe all potential uses and disclosures of patient information and inform patients of their rights under the Privacy Rule. Among these rights is the right for patients to request restrictions on uses and disclosures of their medical information if they so desire.

As can be expected, the required notice of privacy practices was so long that it was unfriendly to patients and consumers. HHS now allows a "layered notice"—a short summary notice that is placed on top of the longer notice containing all the required elements.

Incidental Use and Disclosure Compliance with the Privacy Rule does not eliminate every risk of incidental use or disclosure of PHI. Some incidental uses and disclosures whether or not treatment-related, are permitted. This includes waiting room sign-in sheets, hospital bedside charts, doctors can talk to patients in semi-private rooms and doctors can confer at nurse's stations without fear of violating the rule if overheard by a passerby. However, the covered entity must apply reasonable safeguards, and where applicable, implement the minimum necessary standard. Unfortunately, the final rule does not describe the kinds of safeguards a covered entity is expected to implement to limit incidental disclosures.

Authorization Requirement The authorization requirement required under the draft Privacy Rule has been simplified. Previously, separate authorizations were required for different events depending on the use and/or disclosure anticipated. Patients will still have to grant permission in advance for those disclosures requiring an authorization, but providers will not need to use different types of forms each time.

Minimum Necessary Rule Covered entities and their business associates should not use or disclose protected health information beyond what is reasonably necessary. Minimum necessary principles are meant to be consistent with and not in opposition to, professional judgment. It is apparent, however, that this provision may present an area in which there is some risk of hindsight should an investigation, civil or penal (criminal) action ensue.

*Group $A_{rchaic}$ examined the ramifications of consent and the minimum necessary rule on medical education. The final regulation (2001) noted that a limited amount of patient information can be disclosed to medical, nursing and students of other health professions. In essence, that which can be disclosed is the "minimum required to accomplish teaching." Although provider-to-provider disclosure for treatment is permitted, this means that whenever teaching is involved, a patient signs a one-time consent for use of his/her information in health care operations (including teaching) and providers may condition treatment on consent. However, if the patient (or parent in the case of a minor) refuses, his/her wish is honored. This implies there will be cases "off limits" to medical students and mechanisms will need to be put in place to protect that information from students. During medical rounds, students will need to be excused when the cases of non-consenting patients are discussed. Depending on refusal rates, medical education could suffer.*

*Group members also expressed concern regarding the high cost of fines. We noted the language of HIPAA includes terms such as "reasonable", "professional judgment" and "minumum necessary" and could not help but discern the subjective and retrospective nature of these terms within the law. The extent of exposure and liability posed by HIPAA, and the Privacy Rule in particular, remains to be seen. The federal guidelines appear vague or incomplete in various instances, e.g., what constitutes too much disclosure and how robust "reasonable safeguards" must be. It is hardly comforting to note that the body of case law generated by HIPAA remains to be written.*

*Penalties under HIPAA are substantial and involve **civil and criminal** remedies. Privacy Rule violations are to be enforced by DHHS Office for Civil Rights and include felony conviction and fines of "…not more that $250,000 and/or imprisonment of not more than 10 years". Violations of Administrative Simplification provisions are enforced by CMS (Centers for Medicare and Medicaid). These civil penalties pack hefty financial clout since claims transmissions are often multiple, and the number of transaction standard violations can add up. For example: "…if a provider sends a batch of claims electronically directly to a payer but does not use the 837 formats, the penalties would be $100 for each of the claims in that batch. Assuming the provider sends 100 claims per day, the possible penalty would be $10,000 ($100 x 100 claims)".[5] There is a cap of $25,000 **per standard per year**. If you violate a security standard, a code standard, a unique identifier standard, etc. over the course of a year, the financial repercussions can be extreme.*

Parental Access A covered entity may disclose protected health information about an unemancipated minor to the parents, guardian or other person acting in loco parentis if *the disclosure is permissible under state law*. The covered entity cannot disclose such information if prohibited by state laws. In cases where a minor controls his/her health information and state law is silent regarding a parent's ability to access such information, a provider may exercise his professional judgment, so long as his decision is not inconsistent with applicable law.

Business Associates Covered entities (physicians, hospitals, other health care providers, health plans and clearinghouses) must ensure that any patient information disclosed to business associates (accountants, consultants, billing

companies, etc and other entities that may not be covered by HIPAA) remains protected. Covered entities must enter into or amend written contracts with their business associates and mitigate any harm caused by a known wrongful use or disclosure of patient information made by a business associate.

*Once again, liability and cost were major concerns of Group A$_{rchaic.}$ The AMA notes that these provisions clearly attempt to stretch the regulatory reach of the rule by placing on physicians the burden of regulating the privacy practices of those who fall outside of the rule's reach. This rule requires rewriting or amending existing contracts with business associates on or before April 14, 2004. Where no written contract is in place, covered entities must enter into a business associate agreement, also on or before April 14, 2004.*

*It is clear that covered entities become potentially liable under the Privacy Rule as a result of a breach of patient confidentiality by a business associate. This also places a huge financial burden on covered entities regarding legal and contracting fees. The impact on large health systems, with a plethora of business agreements is substantial. Even so, the economic burden on small health systems and physician practices is clearly disproportionate.*

*Parental Access requires the provider to know, and in essence, balance, the regulatory language of his/her state law with the federal legislation. Unlike the majority of HIPAA directives, this provision will vary state to state and by jurisdiction.*

Limited Data Set The final Privacy Rule sets a new standard for certain uses and disclosures of information that is not completely de-identified, designated as a "limited data set". A limited data set is protected health information that excludes specific, readily identifiable information, not only about the individuals themselves, but also their relatives, employers and members of their households.

The Privacy Rule permits disclosure *without authorization* limited data sets containing admission, discharge and service dates; date of death or birth; age; town, city, state or five-digit zip code; only for research, public health and health care operations purposes. Disclosure of the limited data set would be conditioned on the recipient's written agreement to:

· limit the use of the data set
· limit who can use or receive the data
· and not to re-identify the data or contact patients.

Uses and Disclosures Regarding FDA Products and Research The final Rule permits covered entities to disclose protected health information, without authorization, to a person subject to the jurisdiction of the FDA for public health purposes related to the quality, safety or effectiveness of FDA-regulated products or activities such as collecting or reporting adverse events, dangerous products,

and defects or problems with FDA-regulated products. This is meant to assure that information will continue to be available to protect public health and safety.

Researchers may use a single combined form to obtain informed consent for their research as well as authorization to use or disclose protected health information for such research. Certain transition provisions are in place to prevent needless interruption of ongoing research.

*Group $A_{rchaic}$ examined the impact of these provisions on research and research administrators. There must be de-identification of protected health information (PHI) in archival medical records if information is to be used or disclosed. A total of 18 elements in the medical record require removal to protect health information. Without de-identification, it will be necessary to obtain either consent from patients for use of this archival material or a waiver from the IRB. This rule may be onerous on the conduct of Epidemiologic and health services research, expensive in terms of records keeping and could have a chilling effect on health services research.*

*In terms of granting IRB waivers, regulations require 8 new criteria, some of which are difficult to interpret and may be contradictory. For example one rule requires that the waiver will NOT ADVERSELY AFFECT the privacy rights and the welfare of individuals, whereas another rule requires that the use or disclosure of the information involves no more than MINIMAL RISK to the individual. Another rule requires that privacy risks are reasonable in relation to anticipated benefits. This is a subjective standard that really depends on the personal beliefs and ideologies of individual IRB members.*

*The final Privacy Rule accords patients the right to inspect, copy and **amend** personal medical records. How these "amendments" will impact medical research remains to be seen.*

Conclusion: The Challenges facing Healthcare post HIPAA

It is clear that the Administrative Simplification provisions within HIPAA present both positive and negative ramifications. The overarching goal is the cost reduction and the consistency afforded by standardized EDI (electronic data interface). Decreased administrative overhead and improved operational efficiencies should translate into increased profitability for managed healthcare businesses and providers. The negative impact of the AS provision entails implementing this technology across a multitude of complex systems and platforms while meeting its mandates. Substantial costs will be incurred by states, administrators and providers in order to comply with HIPAA. Costs will reflect system conversions, upgrades, automation start-up, compliance audits and security mechanisms. Human capital will involve additional staffing, training and oversight. In the end, the consumer/patient/taxpayer will also bear these costs.

The benefit to consumers of improved quality and effectiveness in delivery of their healthcare should not be underestimated. Administrative Simplification heralds the ability to promote accuracy, reliability and usefulness as information is shared between healthcare organizations and providers. Technology can provide a cohesive medium as the patient moves through a continuum of healthcare providers, and serves to increase administrative throughput.

At the macro level, implementation of the Privacy Rule presents the greatest challenge for most healthcare organizations. It will also present the most exposure to potential civil and criminal liabilities. Robust risk management and compliance metrics will be critical.

On the micro level, the paradigm shift from confidentiality to privacy, where the patient and not the health care provider, controls the flow of information heralds a transfer of power. This power of information is placed squarely on the consumer. These provisions also promise to trigger major cultural and organizational changes. Government agencies are charged with protecting this newly articulated right.[6]

At first blush, the sweeping nature of HIPAA, and Administrative Simplification in particular, appears at variance with the incrementalism so pervasive in healthcare policy to date. Our text also points to the ambiguous nature of much federal and state health legislation. HIPAA articulates its mandates clearly. Congress has responded to a perceived need in a direct and pressing way.

The destination of HIPAA's ambitious agenda remains unsettled, however. The text continues to change, even if the intent does not. Its provisions crafted by bureaucrats and industry are continually reworked within the democratic process.

For today's healthcare systems, specifically their administrators and providers, HIPAA entails an almost Darwinian challenge—those entities that can adapt rapidly and efficiently will survive. Survival statistics will depend on change, cost and creativity. The ability to change involves transforming not only physical structure and methods, but organizational attitude and culture. Those entities that can shoulder the economic burden presented by HIPAA have a better chance of reaching the end game. HIPAA compels healthcare systems to come into line with trends in other industries. For many reasons, healthcare in the United States has come late to the dance. If nothing else, Administrative Simplification reinforces the notion that healthcare is truly a business.

## References


1. Health Care Financing Administration, "How HIPAA is reshaping the way we do business: The benefits and Challenges of Implementing the Administrative Simplification Standards", Sept. 25, 2000, Vol 1.
2. American Life Project May-June 2000 Poll.
3. Choy, Angela, et al. "E-health: What's Outside the Privacy Rule's Jurisdiction?" Journal of AHIMA 73, no. 5 (2002): 34-39. http://www.ahima.orgHealth Privacy Project Report, "Exposed Online: Why the New Federal Health Privacy Regulation Doesn't Offer Much Protection to Internet Users, Pew Internet & American Life Project. http://www.healthprivacy.org
4. Ibid.
5. Puget Sound Business Journal.
6. Kris Keyes, "The Final HIPAA Privacy Rule", www.imagingeconomics.com.